

Privacy – Online

What You Need to Know About Privacy Issues in 2001

Presented by:

Lynn M. Holmes, Attorney & Counselor-At-Law

Forestville, CA 95436

PH: 707-887-9399 Email: lynn.holmes@usa.net

California State Bar, Business Law Section

Cyberspace Law Committee

September 8, 2001

Personal Identifying Information – Definitions

- Varies from Statute to Statute
 - California Consumer Records: Disposal
 - “Personal information” means any information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, his or her name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver’s license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information.
 - California Identity Theft: Remedies
 - "Personal identifying information" as used in this section, means the name, address, telephone number, driver’s license number, social security number, place of employment, employee identification number, mother’s maiden name, demand deposit account number, savings account number, or credit card number of an individual person.
 - Federal Children’s Privacy Protection Act
 - Personal Information includes: a first and last name, a home or other physical address, an e-mail address or other online contact information, including but not limited to an instant messaging user identifier or a screen name that reveals an individual’s e-mail address, a telephone number, a social security number, a persistent identifier such as a customer number held in a cookie or a processor serial number, where such identifier is associated with individually identifiable information, or information concerning the child or parents of that child that the operator collects online from the child and combines with an identifier described in this definition.
 - European Union
 - Sensitive information includes personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual.

California Consumer Records: Personally Identifying Information

- Pertaining to a particular individual, including, but not limited to
 - his or her name
 - signature
 - social security number
 - physical characteristics or description
 - address
 - telephone number
 - passport number
 - driver's license or state identification card number
 - insurance policy number
 - education
 - employment, employment history
 - bank account number
 - credit card number, debit card number, or any other financial information

Statutes, Regulations, Directives

- State of California

- Constitutional Right of Privacy – As amended in 1972

- Art. I. Sec. 1. All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing and protecting property, and pursuing and obtaining safety, happiness, and privacy.

- Tortious Invasion of Privacy

- Common Law Right of Action

- Appropriation of the plaintiff's name or likeness
 - Intrusion upon the plaintiff's physical solitude or seclusion
 - Publicity placing the plaintiff in a false light in the public eye
 - Public disclosure of true embarrassing private facts

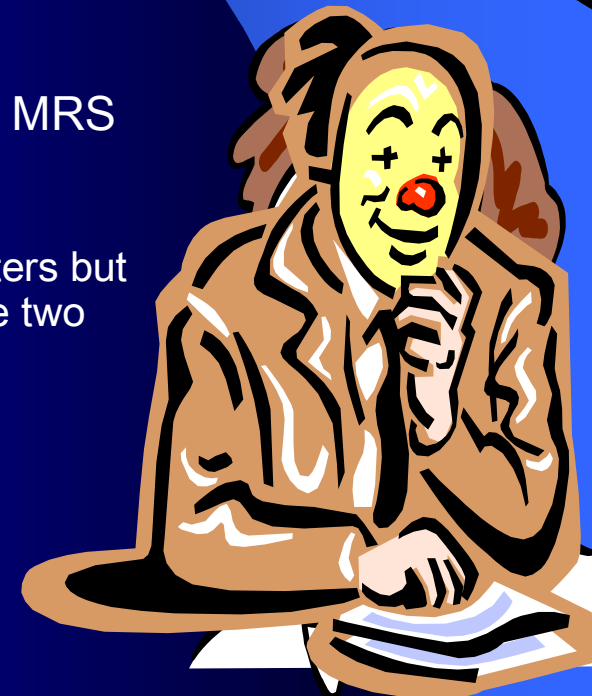
Statutes, Regulations, Directives Cont.

- 6 New Bills signed By Governor Davis – Sept. 2000
 - Disposal of Personal Information
 - Amended Information Practices Act of 1977
 - Requires businesses to take all reasonable steps to destroy or arrange for the destruction of a customer's records within its custody or control containing personal information, which is no longer retained by the business...
 - Office of Privacy Protection (Department of Consumer Affairs)
 - Shall protect the privacy of individuals; personal information in a manner consistent with the California Constitution by identifying consumer problems in the privacy arena.
 - Consumer Credit Reporting: Medical Information
 - Prohibits a consumer-reporting agency from including medical information in reports provided for insurance purposes.
 - Disclosure of Marketing Information by Credit Card Issuers
 - Arias Credit Card Full Disclosure Act of 1986 amended to require the credit card issuer to give consumers an opportunity to opt out annually of having PII shared.

Anonymity Online v. Accountability

Chat Rooms - Bulletin Boards – Message Board Anonymous Users

- ISP must disclose the personal identity of a user upon a court order
 - Notice to user not required
- Anonymous user cases
 - **California: Columbia Ins. Co. v. Seescandy.com**, 185 F.R.D. 573 (N.D. Cal 1999).
 - Identify the missing party with sufficient specificity
 - Identify all previous steps taken to locate the elusive defendant;
 - Establish, to the court's satisfaction, that plaintiff's suit could withstand a motion to dismiss; and
 - File a statement of reasons justifying the specific discovery requested.
 - **New Jersey: Dendrite Int'l v. John Does, et al.**, Docket No. MRS C-129-00, Nov. 23, 2000.
 - New Jersey state court judge utilized the four-part test of Seescandy.com. the judge upheld the anonymity of two posters but ruled Dendrite could subpoena Yahoo! for the identities of the two other posters who did not challenge the subpoenas.
 - Copy of case can be found at <http://www.citizen.org/litigation/briefs/dendrite.pdf>



Statutes, Regulations, Directives Cont.

- Federal

- COPPA -- Children's Online Privacy Protection Act of 1998

- Applies to any site that collects, uses and discloses personally identifiable information (PII) collected from children under 13.

- Notification to Parents.
 - Verifiable Consent From Parents Prior to Collection
 - Child's online activities can NOT be conditioned upon the provision of PII that is not reasonably necessary.
 - Parents must have the right to review, delete and cease the collection of PII from the child upon request.
 - Website must establish policies and procedures to protect confidentiality, integrity, privacy, and security of the information collected.
 - Any material changes to a Sites collection practices requires new consent from parents.

- FTC website provides guidelines compliance:

- <http://www.ftc.gov/bcp/online/edcams/kidzprivacy/index.html>

Statutes, Regulations, Directives Cont.

- Federal

- Gramm-Leach-Bliley Act

- Financial Privacy Act – Disclosure of Nonpublic Personal Information

- Applies to those engaged in
 - “financial activities”
 - “providing data processing and data transmission services, facilities (including data processing and data transmission hardware, software, documentation, or operating personnel), data bases, advice, and access to such services, facilities, or data bases by any technological means, if...[t]he data to be processed or furnished are financial, banking, or economic...”
 - AND serving consumers or customers as defined in the Act
 - Online / Internet Requirements of the Rule: Disclosures on Web Pages:
 - “clear and conspicuous” posting of the privacy policy
 - notice of conspicuous link on a page frequently accessed by consumers, such as the page on which transactions are conducted.

Statutes, Regulations, Directives Cont.

- Federal
 - FTC - Promotes Industry Self Regulation
 - National Advertising Initiative (NAI) Self Regulation Guidelines
 - Online Profiling the collection of information about Internet surfing habits
 - Guidelines for Websites
 - Notice – Consent – Access - Transfer to Third Parties
 - Enforcement
 - Bankruptcy Actions: ToySmart – Questioned the sale of database containing user information where policy statement stated the information would **not be shared** with any third parties.
 - Privacy Seal Providers
 - BBB initiating actions when they determine a site does not comply with FTC regulations

Email – It's Not The USPS

- Workplace Email & Internet Use

- No Expectation of Privacy

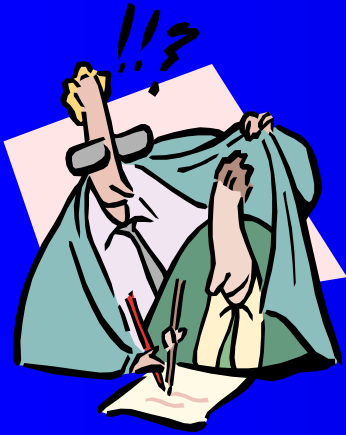
- Workers should be advised to expect NO privacy while using office computers, servers or other equipment.

- Employer may monitor, read and take adverse action against an employee who does not comply with company policy

- NLRB Provides Limited Protection for “Concerted Activities” related to Employment

- IS A CHANGE COMING????

- Administrative Office of U.S. Courts proposes to monitor Federal Judiciary email and internet use



Statutes, Regulations, Directives – Cont.

- Other Countries Choose to Legislate rather than follow the US Approach of Self-Regulation
 - Europe
 - EU Directive: Protection of Personal Data 94/46/EC – Applies to Personally Sensitive Information
 - Each Member Country will enact National Laws furthering the mandates of the Directive.
 - Applies to any company collecting or transferring personal data between countries
 - U.S. Safe Harbor Provisions Agreement in lieu of Regulation
 - Voluntary Registration with FTC
 - Canada
 - Personal Information Protection and Electronic Documents Act
 - Effective January 1, 2001
 - Requires businesses to offer Canadian citizens certain guarantees regarding the collection and use of PII.



Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations (Jan. 2001) Guidelines

- Computer Crime and Intellectual Property Section
Criminal Division United States Department of Justice
 - The law governing electronic evidence in criminal investigations has two primary sources:
 - the Fourth Amendment to the U.S. Constitution, and
 - the statutory privacy laws codified at:
 - Privacy Protection Act, 42 U.S.C. § 2000aa
 - Electronic Communications Privacy Act, 18 U.S.C. §§ 2701-11
 - Title III as modified by the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-22
 - Pen Register and Trap and Trace Devices Statute, 18 U.S.C. §§ 3121-27.
- Guidelines available at:
<http://www.usdoj.gov/criminal/cybercrime/searching.html>

Government Surveillance Systems

Gathering All Email - then sort for the target

- United States
 - Carnivore – Automated system attached to an ISP's to record email
- British System
 - Echelon – automated global interception and relay system
 - Developed under USUK Agreement of 1947 with US-NSA, UK, Canada, Australia & New Zealand
- Russian System
 - Federal Security Service – Monitors internet transmissions in and out of Russia
 - Federal Agency for Government Communications and Information



Lynn m. Holmes,
Attorney & Counselor-At-Law
Phone: 707-887-9399 Email: lynn.holmes@usa.net

- LYNN M. HOLMES, Esq., is an attorney in private practice in Forestville., California. Prior to private practice she had a successful career in semiconductor industry, specifically in sales, contract and international supply line management. She has worked for such companies as National Semiconductor and most recently, International Rectifier. In addition, Ms. Holmes was a principal in a manufacturer's representative organization and represented as a sales agent such companies as Philips Semiconductor, Level One Communications and Maxim Integrated Circuits.
- Ms. Holmes practice is focused on legal issues for business development and transactions, corporations and the Internet. She is an active member of the California State Bar Business Law Cyberspace Law Committee. With the committee she has spoken at various bar meetings on the issues of Online Privacy and Web Agreements. In addition she is a member of the Sonoma County Bar Association, American Bar Association, Sonoma County Women In Law, and North Bay Multi Media Association.